European Commission

This fiche is part of the wider roadmap for cross-cutting KETs activities

'Cross-cutting KETs' activities bring together and integrate different KETs and reflect the interdisciplinary nature of technological development. They have the potential to lead to unforeseen advances and new markets, and are important contributors to new technological components or products.

The complete roadmap for cross-cutting KETs activities can be downloaded from:

http://ec.europa.eu/growth/industry/key-enabling-technologies/eu-actions/ro-ckets

Potential areas of industrial interest relevant for cross-cutting KETs in the Civil Security domain

This innovation field is part of the wider roadmap for cross-cutting KETs activities developed within the framework of the RO-cKETs study. The roadmap for cross-cutting KETs activities identifies the potential innovation fields of industrial interest relevant for cross-cutting KETs in a broad range of industrial sectors relevant for the European economy.

The roadmap has been developed starting from actual market needs and industrial challenges in a broad range of industrial sectors relevant for the European economy. The roadmapping activity has focused on exploring potential innovation areas in terms of products, processes or services with respect to which the cross-fertilization between KETs can provide an added value, taking into account the main market drivers for each of those innovation areas as well as the societal and economic context in which they locate.

Taking the demand side as a starting point, cross-cutting KETs activities will in general include activities closer to market and applications. The study focused on identifying potential innovation areas of industrial interest implying Technology Readiness Levels of between 4 and 8.

SEC.1.2: Cyber security

Scope:

To develop tools and techniques for the cyber security including wireless security, cloud security and privacy, and autonomic network defence.

Demand-side requirements (stemming from Societal Challenges) addressed:

- Contribute to achieving “inclusive, innovative and secure societies”

Demand-side requirements (stemming from market needs) addressed:

- Guarantee border security, considering land, maritime and country borders
- Guarantee security of people including of operators
- Guarantee privacy

Specific technical / industrial challenges (mainly resulting from gaps in technological capacities:

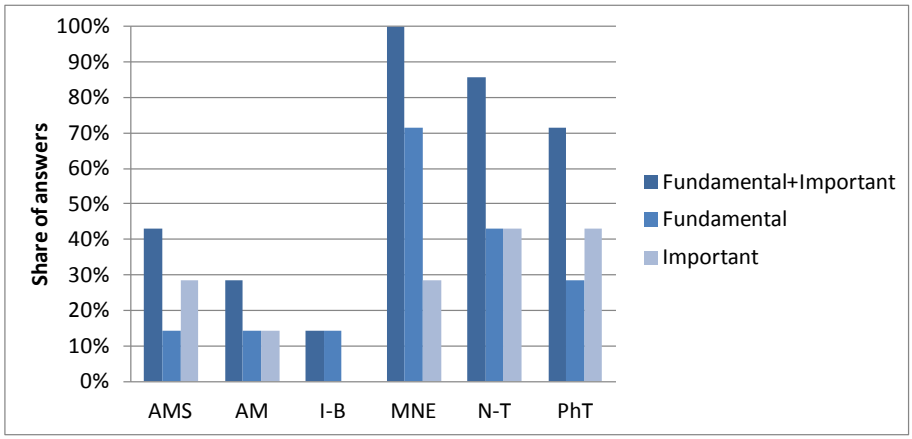
- Development of secure spectrum sharing techniques
- Development of secure operating systems for commercial cellular handsets
- Development of approaches to provide security and privacy for the growing enterprise cloud computing market
- Development of new tools and techniques to secure virtual machines
- Development of proactive network defences that can autonomically implement protective measures against identified attacks

Contribution by cross-cutting Key Enabling Technologies:

In respect to this Innovation Field, the integration of KETs could contribute to the development of more advanced tools and techniques for the cyber security, including wireless security, cloud security and privacy, and autonomic network defence, including low cost, low power, highly secure hardware-based cryptographic protection of networks, limitation of intrusion using near field communication, device-to-device communication, secure protocols and low power consumption integrity validity check.

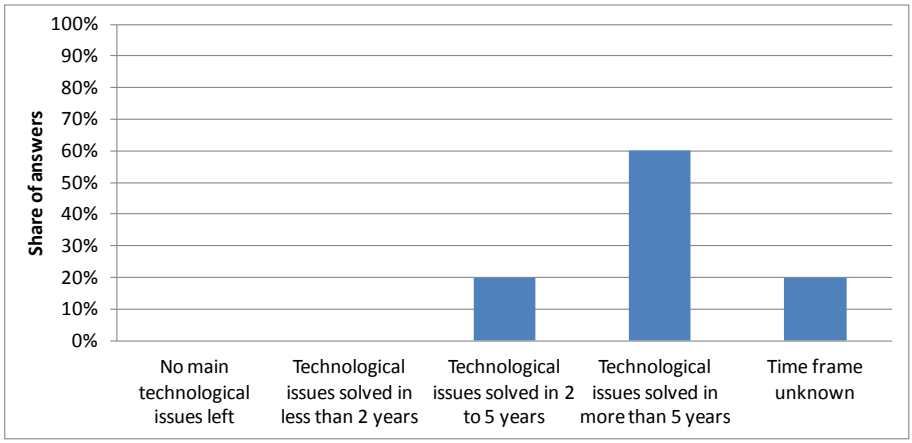
To this aim, the combination of KETs experts’ opinions collected through the dedicated survey (whose result is depicted in the below bar chart), the examination of KETs-related patenting activity in respect to this Innovation Field, and desk research activities, have allowed identifying a rather strong interaction of KETs with respect to this Innovation Field, with either fundamental or important contribution mainly by the following KETs:

- Micro- and Nano-Electronics (MNE)
- Nanotechnologies (N-T)
- Photonics (PhT)
- To a lesser extent, Advanced Manufacturing Systems (AMS) and Advanced Materials (AM)



Timing for implementation:

According to the majority of KETs experts' opinions (whose result is depicted in the below bar chart), desk research, and in line with the KETs-related patenting activity in this field, it is considered that the main technological issues holding back the achievement of cross-cutting KETs based products related to this Innovation Field could be solved in a time frame of more than 5 years:



Hence, depending on the specific technical and/or industrial challenges holding back the achievement of cross-cutting KETs based products related to this Innovation Field, the provision of support in the medium term should be taken into consideration within this framework.

Additional information according to results of assessment:

- ***Impact assessment:***
  - Cyber security market is an amalgamation of various categories of technologies, and services, applied at various levels to protect an organization and user's personal and professional data from cyber threats. The dependence on information and communication technology is the prominent feature of today's modern and interconnected society and economy. The government, public utilities, and enterprises are dependent on internet, wireless and cloud-based services. With this dependency, cyber attacks have shown an exponential increase in the past few years and have generated the need for unified cyber security solutions to support the enhanced enterprise mobility and strict data disclosure laws. The market for security portfolios such as data encryption, authentication, security and vulnerability management, DDoS (Distributed Denial-of-Service) mitigation along with various others are experiencing a boom phase because of an increase in need for a secure and resilient cyberspace. The rapid adoption of cloud computing, data centres, and wireless communication, strict government compliances on data privacy, increasing threat in public utilities along with the rapid increase in sophistication of cyber attacks demand for integrated cyber solutions are expected to create extensive market opportunities for the cyber security solution vendors during the next years, with a market forecast to reach a value of 114 billion Euro by 2019.
  - Source: Markets and Markets, Cyber Security Market (IAM, Encryption, DLP, Risk and Compliance Management, IDS/IPS, UTM, Firewall, Antivirus/Antimalware, SVM/SIEM, Disaster Recovery, DDoS Mitigation, Web Filtering, Security Services) - Global Advancements, Forecasts & Analysis (2014-2019), 2013, www.marketsandmarkets.com
  - With a greater dependence on computer systems and a reliance on integrated networking, today's armed forces are faced with an ever-changing set of challenges in maintaining cyber security from the threat of attack. Rapid evolution in technology has forced governments and industry alike to continually develop secure systems that remain one step ahead of the enemy. As cyber systems become increasingly integrated the requirement for a multi-layered, adaptive and self-learning security system becomes imperative. This innovation field, on which the military and defence knowledge is already quite advanced, could prove useful for also civilian applications related to security, illustrating its dual use potential.
- ***Results of patents scenario analysis:***
  - 1 patent identified in the period 2001-2011 for the specific Innovation Field in relation to KETs
  - No significant patent-related indicators can be reported in this field